

32. The recording medium of claim 22, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

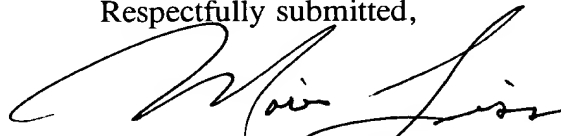
### REMARKS

Claims 1-32 remain in the application. By the foregoing amendment, claims 19 and 26 were amended to eliminate improper multiple dependencies. New claims 31 and 32 are the recitations of claims 19 and 26, respectively, which were eliminated by the foregoing amendment. These changes are not believed to introduce new matter, and entry of this amendment is respectfully requested.

### DEPOSIT ACCOUNT AUTHORIZATION

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary, then such extensions of time are hereby petitioned under 37 CFR § 1.136(a), and any fees required for consideration of this paper, including fees for net addition of claims, are hereby authorized to be charged to our Deposit Account No. 22-0185.

Respectfully submitted,



Morris Liss, Reg. No. 24,510  
Pollock, Vande Sande & Amernick, R.L.L.P.  
1990 M Street, N.W.  
Washington, D.C. 20036-3425  
Telephone: 202-331-7111

Date: 2/2/00